NEWS FROM ED MARKEY

United States Congress Massachusetts Seventh District

FOR IMMEDIATE RELEASE
October 20, 2003

CONTACT: Jeff Duncan
or Colin McCormick
(202) 225-2836

REP. MARKEY DEMANDS BETTER CYBER SECURITY AT NUCLEAR POWER PLANTS

Plant infection highlights computer vulnerabilities at nuclear power plants

WASHINGTON, DC - Representative Edward Markey (D-MA), Senior Member of the Select Committee on Homeland Security and Ranking Member on the Telecommunications and the Internet Subcommittee today released a letter to Nils Diaz, Chairman of the Nuclear Regulatory Commission, urging improved cybersecurity at the nation's 104 licensed nuclear power plants.

"I am concerned that nuclear power plants across the country may be vulnerable to computer viruses and computer hacking," Rep. Markey said. "The safety of these plants depends on their computer systems, which could be targeted by cyber terrorists."

The Nuclear Regulatory Commission (NRC) oversees safety and licensing of U.S. nuclear power plants. On January 25, 2003, the Davis-Besse nuclear plant operated by FirstEnergy Corp. in Oak Harbor, Ohio was infected with the "Slammer" worm computer virus. Two computer systems at the plant were disabled for over four hours. The infection occurred because the plant had a backdoor T1 network connection that bypassed the standard network firewall. The Slammer worm attacked the plant's Microsoft SQL 2000 server, and successfully infected it because plant computer engineers had failed to install a security patch made available six months prior to the attack.

An earlier letter from Rep. Markey to Chairman Diaz on August 22, 2003 asked for information about the NRC's plans to improve nuclear cybersecurity in light of the Davis-Besse situation and press reports indicating that computer problems at FirstEnergy may have played a role in the August 14, 2003 blackout. One week after Markey's letter, and more than six months after the Slammer worm hit the Davis-Besse facility, the NRC issued a notice to other licensees alerting them to the threat posed by the virus. Chairman Diaz replied that the NRC is conducting "pilot studies" of cybersecurity at four nuclear plants, and is consulting with the Nuclear Energy Institute, an industry organization, to develop guidelines. However, the NRC did not indicate whether the Commission has coordinated its efforts with other government agencies with expertise in cybersecurity, such as the Department of Homeland Security's National Cyber Security Division, or consulted with any non-nuclear industry cyber security experts. The NRC has also not required that network connections to nuclear plant computers go through a firewall or that security patches be installed promptly.

Rep. Markey concluded, "We face an array of threats to our security in the post-September 11 world, and cyber terrorism is one of them. Simple steps, like making sure that all network connections to a nuclear plant go through a firewall, or that nuclear plant computer engineers quickly install security patches, could do a lot to help. But we also need to develop a comprehensive, clear and effective plan for nuclear plant cyber security, with input from government, industry and independent experts. Otherwise our nuclear power plants are sitting ducks for hackers, or worse, for terrorists."

Additional information is available at Rep. Markey's website, http://www.house.gov/markey.